UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/775,758	02/09/2004	Woodrow A. Thrower	SYMAP040	8711

21912 7590 06/16/2008

VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

EXAMINER	
BROWN, CHRISTOPHER J	
ART UNIT	PAPER NUMBER
2134	
MAIL DATE	DELIVERY MODE
06/16/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/775,758	THROWER ET AL.	
	Examiner	Art Unit	
	CHRISTOPHER J. BROWN	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 February 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8 and 12-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8, 12-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

Applicant's arguments, filed 2/28/2008, with respect to the rejection(s) of claim(s) 1-8, 12-21 under USC 102 have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Liang US 2004/0205419 who teaches a responsive action in real-time to control a detected threat agent.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-8, 12-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cohen US 6,952,779 in view of Liang US 2004/0205419.

As per claims 1, and 21 Cohen teaches identifying a threat agent (attacker) having an existing access level (having access to web server 246) (Col 6 lines 5-7, lines 20-25). Cohen teaches using the existing access level to analyze an attack path between the threat agent and an asset (start and end points for attack path) (Col 6 lines 48-54, Col 7 lines 1-

7). Cohen teaches updating the existing access level if the analysis of the attack path between the threat agent and the asset indicates that an attack along the path would be successful (implementing fixes to deprive attackers from being able to access the asset) (disabling DDE, patching servers, disabling rlogin access,)(Col 9 lines 35-40, Col 17 lines 10-23). Cohen teaches analysis of the attack path between the threat agent and the asset indicates that an attack along the path would be successful comprises updating the existing access level to include the resulting access level if it is determined that the threat agent has used or could use the exploit (if the threat is successful in exploiting a vulnerability the existing access level, web server access, is updated to the resulting access level, access to admin and application servers). (Fig 5, Col 14 table, Col 15 lines 48-61) . Cohen teaches iteratively (scheduled frequencies) updating the existing access level (access to web server) (Col 10 lines 35-40, 53-60, 62-67, Col 11 lines 40-50). Cohen teaches determining that no further attack along the attack path would be successful if there are no further exploits (buffer overflow attack) associated with the asset for which the existing access (web server access) of the threat agent (attacker, is updated to reflect any resulting access (access to admin or application server) that has been or would be attained from the successful completion of previously-analyzed exploits (buffer overflow exploit), is greater than or equal to the prerequisite access (web server access) associated with the exploit. (checking all possible attack routes with systems that runs repeatedly to analyze the system, fix/patch and analyze again in an iterative pattern) (Col 10 lines 35-40, 53-60, 62-67, Col 17 lines 8-22).

Liang teaches in the event it is determined that an asset would be reached by the threat agent, taking a responsive action in real time prior to the asset being reached by the threat agent, including implementing a control or countermeasures (detecting virus and implementing actions for preventing computer viruses from damaging the files in the network, including isolating the network node and preventing traffic into the node).

It would have been obvious to one of ordinary skill in the art to use the rapid response of Liang with the threat analysis and security updated of Cohen because it would allow fixes in a rapid manner to prevent damage from any detected attack.

As per claim 2, Cohen teaches using the existing access level to analyze an attack path between the threat agent and an asset comprises identifying a vulnerability associated with the asset (identifying vulnerabilities) (Col 2 line 60).

As per claim 3, Cohen teaches using the existing access level to analyze an attack path between the threat agent and an asset comprises identifying an exploit method associated with a vulnerability associated with the asset (calculating attacks, exploits and targets) (Col 9 lines 8-17)

As per claim 4, Cohen teaches the exploit method has associated with it a prerequisite access level (precondition, access to web server 246) required to use the

exploit method to exploit the vulnerability successfully (teaches the exploit has access that will be used to exploit vulnerability, such as using buffer overflow attack to access web server 246) (Col 14, table, Col 15 lines 54-61) .

As per claim 5, Cohen teaches using the existing access level to analyze an attack path between the threat agent and an asset comprises comparing the existing access level to the prerequisite access level (analyze attack path using existing access level to collect preconditions and exploit them) (Col 13 line 18 to Col 14 line 18).

As per claim 6, Cohen teaches determining whether a control affects the prerequisite access level (determining whether a server patch or firewall affects access level) (Col 17 lines 10-15).

As per claim 7, Cohen teaches the exploit has associated with it a resulting access level (access to administration server 254, or application server 262) that may be attained by using the exploit to exploit the vulnerability successfully (gaining control of web server to further gain access to other servers using exploits) (Fig 5, Col 14 table, Col 15 lines 48-61) .

As per claim 8, Cohen teaches determining whether a control affects the prerequisite access level (determining whether a server patch or firewall affects access level) (Col 17 lines 10-15).

As per claim 12, Cohen teaches determining whether the asset is subject to compromise by the threat agent (attack simulation and determined consequences)(Col 8 lines 7-15).

As per claim 13, Cohen teaches determining whether a control affects the existing access level of the threat agent (preventing buffer overflows by patching web servers) (Col 17 lines 13-20)

As per claim 14, Cohen teaches updating the existing access level (access to web server 246) to reflect the affect of the control prior to using the existing access level to analyze an attack path between the threat agent and an asset (fixing the buffer overflow exploit with a patch (control), and retesting to determine attack success between agent and asset) (Col 10 lines 35-50, Col 17 lines 13-20).

As per claim 15, Cohen teaches receiving from a network security system or application data comprising an identification of the threat agent (identifying possible attacks) (col 7 lines 5-10).

As per claim 16, Cohen teaches receiving from a network security system or application data that may be used to identify the threat agent (data collected by discovery agents) (Col 10 lines 43-46).

As per claim 17, Cohen teaches providing output data reflecting a result of the analysis of the attack path (generates a list of attacks) (Col 10 lines 49-53).

As per claim 18, Cohen teaches a report of the highest level of access that has been or could be achieved by the threat agent through one or more attacks along the attack path (calculates endpoints including ultimate endpoints, and damage through attack path) (Col 8 lines 30-55).

As per claim 19, Cohen teaches using the existing access level further includes evaluating recorded data to determine the attack path (teaches evaluating data collected and recorded about vulnerabilities and attack simulations) (Col 10 lines 40-50).

As per claim 20, Cohen teaches the attack path is determined by computing a transitive closure (checking possible paths) (Col 7 lines 1-8).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CHRISTOPHER J. BROWN whose telephone number is (571)272-3833. The examiner can normally be reached on 8:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571)272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christopher J Brown/ 6/13/08

Primary Examiner, Art Unit 2134